Claims 1, 2, and 4-19 are pending in this application. The specification was objected to. Claims 1, 2, 4-11, and 17-19 were rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. patent 5,640,456 to Adams, Jr. et al. (herein "Adams") in view of "A Solution to Wireless Connections in a Multi-Bus Network" to Sato et al. (herein "Sato") and further in view of "5C Digital Transmission Content Protection White Paper" to Hitachi et al. (herein "Hitachi"). Claims 12 and 13 were rejected under 35 U.S.C. § 103(a) as unpatentable over Adams in view of U.S. patent 5,175,765 to Perlman and further in view of Hitachi. Claims 14 and 16 were rejected under 35 U.S.C. § 103(a) as unpatentable over Adams in view of Hitachi.

Addressing first the objection to the specification, the specification is believed to be in full compliance with all requirements.

The specification was objected to as not providing a description for "converted data, nor another coding format" of claim 17.

In response to that objection applicants' note Figure 44 in the present specification, and particular at step S6518, shows a conversion, and see also the present specification at page 56, lines 17-19. Such disclosures are believed to fully support the noted conversion of claim 17.

Addressing now the above-noted prior art rejections, those rejections are traversed by the present response.

Each of the above-noted rejection cites Adams as a primary reference. However, applicants submit that Adams does not teach features relied upon in the rejection, Adams could not be properly modified in any manner to meet the claim limitations, and further no combination of teachings of Adams in view of Sato and Hitachi, or in view of Perlman and Hitachi, or in view of Hitachi, would fully meet the claim limitations.

Adams discloses an encryption/decryption device, which is to be spliced in a single local area network.

Adams first differs from the claims in that Adams is not directed to a device between two networks operated under different protocols, as recognized in the Office Action.[1]

To overcome the above-noted recognized deficiencies in Adams, the outstanding Office Action cites the teachings in Sato. However, applicants note such a modification is believed to be clearly improper as it makes no sense to modify Adams to be placed between two networks as Adams is specifically designed for a single local area network.

The Office Action also recognizes that the combination of Adams and Sato fails to disclose carrying out a contents protection procedure including at least an authentication and/or a key exchange between one device/service/sub-unit on a first network and another device/service/sub-unit on a second network.[2]

In response to that basis for the outstanding rejection, as Adams does not disclose anything related to a contents protection procedure to begin with, the teachings in Hitachi make no sense whatsoever in combination with the teachings in Adams.

Addressing the above points in further detail, Adams discloses an encryption/decryption device that is to be spliced in a single local area network, and that selectively encrypts or decrypts only a data portion of a data packet, leaving routing information contained in the header and trailer portions of the data packet unchanged (see the Abstract of Adams).

The claims as currently written are not directed to such an encryption/decryption device as in Adams that selectively encrypts/decrypts only a data portion, without encrypting/decrypting routing information in a header.

---

[1] Office Action of March 4, 2004, page 4, lines 11-12.
[2] Office Action of March 4, 2004, the sentence bridging pages 4 and 5.

In contrast to Adams, the claims are directed to a relay device that handles contents protection information that is necessary in carrying out a contents protection procedure including at least an authentication and/or a key exchange between one device/service/sub-unit on a first network and another device/service/sub-unit on a second network, or a relay device that carries out a contents protection procedure including at least an authentication and/or a key exchange, separately with respect to one device/service/sub-unit on the first network and with respect to another device/service/sub-unit on the second network.

With respect to the above-noted claim features, Adams completely fails to teach or suggest any contents protection procedure including at least an authentication and/or a key exchange. The basis for the outstanding rejection appears to be confusing the encryption/decryption in Adams with the "contents protection procedure" in the claims. In that respect, applicants note that authentication and/or key exchange are procedures to be carried out between two nodes that wish to communicate with each other, for authenticating each other or sharing a key to be used for the encryption/decryption. The contents protection procedures themselves do not encrypt/decrypt anything, and thus are distinct from the encryption/decryption such as in Adams.

The basis for the outstanding rejection also cites specifically teachings in Adams at column 4, lines 40-52; column 5, lines 2-5; column 5, line 61 to column 6, line 5; column 6, lines 6-16 and 21-29; and column 6, line 65 to column 7, line 11 with respect to the claimed "contents protection procedure" features.

With respect to those indications in the Office Action, applicants first note that at column 4, lines 40-52 Adams only discloses a table to be used in making a routing or encryption/decryption decision, that includes keys for encrypting and decrypting data. Such teachings in Adams clearly fail to even address any authentication and/or key exchange. Further, at column 5, lines 2-5 Adams merely discloses an upstream port and a downstream

port, and that portion of Adams also clearly fails to even address any authentication and/or key exchange. Further, at column 5, line 61 to column 6, line 5 Adams merely discloses that a header includes a source and destination, checksums, and option bits such as that which indicate that data are encrypted. Such a disclosure in Adams, however, also clearly fails to even address any authentication and/or key exchange. Further, at column 6, lines 6-16 Adams merely discloses extraction of header information and comparison of the extracted header information with a key list at the time of the encryption, at column 6, lines 21-29 Adams merely discloses that a key list contains keys for encrypting/decrypting data and handling information, and at column 6, line 65 to column 7, line 11 Adams merely discloses reconstruction of IP data packet using the encrypted data. The above-noted portions of Adams also clearly fail to teach or even address any authentication and/or key exchange.

In such ways, Adams completely fails to disclose or suggest any features or operations related to the claimed features of a contents protection procedure including at least an authentication and/or key exchange. Thereby, Adams fails to disclose or suggest any elements corresponding to the "contents protection information reception unit" and "contents protection information transfer unit" of claims 1 and 2, the "first contents protection unit" and the "second contents protection unit" of claims 5, 11, and 19, the "copy protection processing unit" of claims 12, 13, 14, and 16, and the "first copy protection processing unit" and the "second copy protection processing unit" of claim 17.

Moreover, applicants note the relay device of claim 1 can operate to "transparently" relay contents protection information, without making any change, while relaying the control command signals "non-transparently". Adams clearly fails to disclose or suggest any relay device that selectively relays only the contents protection information "transparently". It is noted here that the relay device of the present invention is described as "transparent" when

certain information is simply passed through the relay device without making any change to the certain information.

Similarly, the relay device of claim 2 "transparently" relays the contents protection information and the protected (encrypted) contents, without making any change thereto, while it relays the control command signals "non-transparently". Adams clearly fails to disclose or suggest any relay device that selectively relays only contents protection information and encrypted contents "transparently".

Moreover, the relay device of claim 5 carries out a contents protection procedure including at least authentication and/or key exchange, separately with respect to the device/service/sub-unit on the first network and the device/service/sub-unit on the second network, and further the relay device of claim 5 receives the encrypted contents from one network side and re-encrypts the contents at the time of transferring the contents to the other network side. Adams clearly fails to disclose or suggest any relay device that carries out contents protection procedures separately and re-encrypts the contents at the time of the contents transfer.

Similarly, the relay device of claim 11 carries out the contents protection procedure including at least the authentication and/or the key exchange separately with respect to the device/service/sub-unit on the first network and the device/service/sub-unit on the second network, by using identical key information, and the relay device of claim 11 receives the encrypted contents from one network side and re-encrypts the contents at the time of transferring the contents to the other network side. Adams clearly fails to disclose or suggest any relay device that carries out contents protection procedures separately by using identical key information and that re-encrypts the contents at the time of the contents transfer.

Similarly, the relay device of claim 17 carries out the contents protection procedure including at least authentication and/or key exchange separately with respect to the

device/service/sub-unit on the first network and the device/service/sub-unit on the second network, and that relay device receives the encrypted contents from one network side, converts its coding format, and re-encrypts the contents at a time of transferring the contents to the other network side. Adams clearly fails to disclose or suggest any relay device that carries out a contents protection procedure separately, converts the coding format of the received contents, and re-encrypts the contents at the time of the contents transfer.

Similarly, the relay device of claim 19 carries out the contents protection procedure including at least authentication and/or key exchange separately with respect to the device/service/sub-unit on the first network and the device/service/sub-unit on the second network, by referring to states of the contents reception unit and the contents transmission unit, and that relay device receives the encrypted contents from one network side and re-encrypts the contents at the time of transferring the contents to the other network side. Adams clearly fails to disclose or suggest any relay device that carries out a contents protection procedure separately by referring to states of the contents reception unit and the contents transmission unit, and that re-encrypts the contents at the time of the contents transfer.

In such ways, the teachings in Adams are significantly deficient with respect to the claimed features, and Adams does not disclose each of the claimed features as relied upon in the basis for the outstanding rejections. Moreover, no teachings in Sato or Hitachi can overcome the above-noted deficiencies in Adams. Further, Adams is clearly directed to use in a single local area network and cannot be properly modified to meet the claim limitations in any manner.

In such ways, no combination of teachings of Adams in view of Sato and further in view of Hitachi renders obvious the subject matter of independent claims 1, 2, 5, 11, 12, 13, 14, 16, 17, and 19, or any of the claims dependent therefrom.

Moreover, additional features recited in certain of the claims noted above even further distinguish over the applied art as now discussed below.

The communication device of claim 12 receives an authentication target query (a query regarding a service/sub-unit/plug that is transferring the encrypted contents) from another device, and returns an authentication target reply (notifies a service/sub-unit/plug that it is transferring the encrypted contents) to the another device in response.

Further, the communication device of claim 13 transmits an authentication target query (a query regarding a service/sub-unit/plug that is transferring the encrypted contents) to another device, and receives an authentication target reply (notification regarding a service/sub-unit/plug that it is transferring the encrypted contents) from that another device in response.

With respect to claims 12 and 13, the Office Action correctly indicates that Adams fails to disclose or suggest such features regarding the authentication target query and reply. To overcome such deficiencies in Adams the Office Action cites the teachings in Perlman at column 14, lines 38-49.[3]

However, in that respect applicants note Perlman at column 14, lines 38-49 merely describes a query from a network manager to each node to determine if the node receives a particular packet. Such a disclosure in Perlman completely fails to disclose or suggest any query and reply regarding a service/sub-unit/plug that is transferring encrypted contents, particularly to ascertain which service/sub-unit/plug is transferring the encrypted contents. Thus, the teachings in Perlman cannot overcome the deficiencies of claims 12 and 13.

Moreover, Adams also fails to disclose or suggest the "copy protection processing unit" of claims 12 and 13 as discussed above.

[3] Office Action of March 4, 2004, page 23, first paragraph.

In such ways, applicants respectfully submit that claims 12 and 13 further distinguish over the applied art to Adams in view of Perlman and Hitachi.

With respect to the rejection of claims 14-16, the communication device of claim 14 transmits or receives encrypted contents through a flow, and carries out the contents protection procedure including at least an authentication and/or a key exchange in units of the flow.

The Office Action indicates that such features are disclosed by Adams at column 4, lines 40-44; column 5, line 65 to column 6, line 5; and column 6, lines 17-20 and 21-29.[4]

However, with respect to those teachings in Adams, at column 4, lines 40-52 Adams merely discloses a table to be used in making a routing or encryption/decryption decision, which includes keys for encrypting and decrypting data. Such a disclosure in Adams completely fails to disclose or suggest any flow as well as any authentication and/or key exchange.

At column 5, line 65 to column 6, line 5 Adams merely discloses that a header includes a source and destination, checksums, and option bits such as that which indicate that the data are encrypted. However, that portion of Adams also clearly fails to disclose or suggest any flow as well as any authentication and/or key exchange.

At column 6, lines 17-20 Adams merely discloses that a key list contains matching criteria such as source addresses and destination addresses. That disclosure in Adams also fails to disclose or suggest any flow as well as any authentication and/or key exchange. Moreover, at column 6, lines 21-29 Adams merely discloses that a key list contains keys for encrypting/decrypting data and handling information. That disclosure in Adams also fails to disclose or suggest any flow as well as any authentication and/or key exchange.

[4] Office Action of March 4, 2004, page 26, last paragraph.

Hitachi also fails to teach or suggest the above-noted features. In such ways, claims 14 and 15 also clearly distinguish over the teachings in Adams and Hitachi.

Further with respect to claim 16, in the communication device of claim 16 at least one of an identifier of a service, a sub-unit, a virtual channel, or a plug and an identifier for uniquely identifying encrypted contents is attached to information exchanged in the contents protection procedure including at least an authentication and/or a key exchange.

The outstanding rejection cites Adams at column 4, lines 40-52 and column 5, line 61 to column 6, line 5 to meet such limitations.[5] However, such teachings in Adams do not meet such claim limitations as now discussed.

At column 4, lines 40-52 Adams merely discloses a table to be used in making a routing or encryption/decryption decision, which includes keys for encrypting and decrypting data. Such a portion in Adams clearly fails to even address any identifier of a service, a sub-unit, a virtual channel, or a plug or identifier for uniquely identifying the encrypted contents, as well as any authentication and/or key exchange. Further, at column 5, line 61 to column 6, line 5 Adams merely discloses that a header includes a source and destination, checksums, and option bits such as that which indicates that data are encrypted. Such a disclosure in Adams clearly fails to disclose or suggest any identifier of a service, a sub-unit, a virtual channel, or a plug or identifier for uniquely identifying encrypted contents, as well as failing to disclose any authentication and/or key exchange.

In such ways, claim 16 also clearly distinguishes over the combination of teachings of Adams in view of Hitachi.

In view of these foregoing comments, applicants respectfully submit that the claims as currently written clearly distinguish over the applied art.

[5] Office Action of March 4, 2004, pages 28-29, prenumbered point 24.

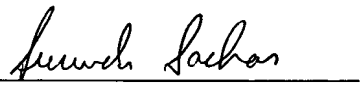
As no other issues are pending in this application, it is respectfully submitted that the present application is now in condition for allowance, and it is hereby respectfully requested that this case be passed to issue.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)



Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870
Surinder Sachar
Registration No. 34,423

EHK:SNS\la

I:\ATTY\SNS\0039\00397378\00397378-REQ RECON DUE 090404.DOC